



A study on the approximate GCD

著者	讃岐 勝
内容記述	Thesis (Ph. D. in Science)--University of Tsukuba, (A), no. 4555, 2008.3.25 "February 2008"--Cover Includes bibliographical references (leaves 50-54)
発行年	2008
URL	http://hdl.handle.net/2241/111075

氏 名 (本籍)	讃岐勝 (北海道)
学 位 の 種 類	博 士 (理 学)
学 位 記 番 号	博 甲 第 4555 号
学位授与年月日	平成 20 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
審 査 研 究 科	数理解物質科学研究科
学 位 論 文 題 目	A Study on the Approximate GCD (近似 GCD に関する研究)
主 査	筑波大学教授 理学博士 佐々木 建 昭
副 査	筑波大学教授 博士 (理学) 青 嶋 誠
副 査	筑波大学教授 理学博士 笠 原 勇 二
副 査	筑波大学准教授 理学博士 坂 井 公

論 文 の 内 容 の 要 旨

本学位論文は、浮動小数を係数とする多項式の近似 GCD に関して、1) 1 変数多項式の剰余列算法を安定化した算法の提案、2) 多変数多項式に対する PC-PRS 算法の近似化、3) 種々の悪条件な場合に対する工夫、の三つの研究をまとめている。

1980 年代末に Sasaki 等により切り開かれた近似代数の研究は、今では計算代数の世界的トピックスとなった。その中で、近似 GCD (最大公約子) は最もよく研究されたテーマであるが、現在でも活発に研究されている。近似代数では、与式に未知の摂動項を仮定して演算を定義するが、実際計算では数係数を浮動小数として扱うことが多い。そのため、厳密計算では生じない問題が生じる。その代表が計算の不安定性である。誤差のみからなる項が生じて計算結果が無意味なものになったり、桁落ちと呼ばれる現象により計算結果の精度が大幅に低下するのである。

本論文では、誤差のみからなる項の除去に関しては、そのような誤差項に対処するため Kako-Sasaki が考案し、国産数式処理システム GAL に実装した“有効浮動小数”の利用を提案している：数係数を有効浮動小数で表すだけで誤差のみからなる項が自動的に除去される。その簡単さと有効さゆえ、有効浮動小数は世界的商用システム Maple への搭載が決まった。桁落ちの回避に関しては、現在の世界の潮流は数値計算で考案された行列算法を転用することだが、本論文では昔ながらの剰余列算法の安定化を研究した。

1 変数多項式の剰余列算法の改善。浮動小数係数の多項式剰余列を計算すると多くの場合、桁落ち誤差が次々と積もり、昔ながらの算法は高次多項式には使えない。桁落ちの原因は二つある：第一は与式または途中式に微小 (巨大) 主係数が現れる場合で、第二は与式が近接根を含む場合である。大きな許容度でみれば近接根は近似公約子に含まれるので、第二の場合は近接根どうしが分離されるまで剰余列を計算するときに問題となるが、この場合に対しては多くの方法が考案されている。本論文では第一の場合を扱っている。微小主係数多項式による剰余列計算での桁落ちは、数値行列のガウス消去における桁落ちと類似である。数値行列ではピボティング (行を入れ換えて先頭要素が大きい行で消去を行う) という操作で劇的に桁落ちが消えるが、本論文は同様の操作で桁落ちを除くことを提案している。具体的には、除多項式の主係数が微小

な場合、除多項式と被除多項式の役割を入れ換えて剰余列を生成するのであるが、垂直にこれを行うと定数項に悪条件性が移動するので、それを防ぐ工夫を行っている。著者はこの方法を、現在最も安定な方法と言われている QRGCD 算法 (Sylvester 行列の QR 分解に基づく方法) と比較した。その結果、効率でははるかに勝るものの、精度の点では到底及ばず、特に 50 次以上の多項式ではまだまだ改良の必要があると報告している。

多変数多項式に対する PC-PRS 算法の近似化。整係数多変数多項式の GCD 計算では、計算効率の観点から見て、Moses-Yun の EZ-GCD 算法 (Hensel 構成を利用) と Sasaki-Suzuki の PC-PRS 算法 (従変数部分をべき級数とみなし、高次項をカットしつつ剰余列を計算する) が双壁である。本論文は、PC-PRS 算法を浮動小数係数用に近似化した算法を提案し、他の代表的算法と比較して、著者の提案した算法の優越性を実験的に立証した。悪条件の場合を除けば、近似化自体は容易である。比較した算法は 2004 年にアメリカの二つのグループが提案したもので、どちらも Sylvester 行列に基づく 1 変数多項式用の算法を多変数化したものである。多変数多項式用の一般 Sylvester 行列は計算で現れ得る全ての単項式を台とするため、変数の個数が多いほど巨大な行列となり、必然的に近似 GCD の計算に巨大なメモリを必要とし時間がかかる。一方、近似 PC-PRS 算法は、PC-PRS 算法の効率性をそのまま受け継いで非常に効率がよい。著者はさらに、近似 PC-PRS 算法を、EZ-GCD 算法を近似化した算法とも比較した。その結果、Hensel 構成の初期因子が近接根を持つ場合に近似 EZ-GCD 算法は精度低下を起こすが、近似 PC-PRS 算法はより安定であることを実験的に実証した。

三つの悪条件な場合に対する工夫。数値行列で、行あるいは列の間に近似線形従属性が成立する場合は悪条件と言われ、ピボティングを行っても桁落ちは残る。同様に近似 GCD 計算においても悪条件な場合がある。1) 近似 GCD の主係数が微小な場合、2) 巨大主係数が現れる場合、3) 与えられた多変数多項式の主係数の定数項が微小な場合、などである。本論文では、これら三つの場合にそれぞれ安定化法が提案されている。

1) GCD の主係数が微小な場合は、QRGCD その他の方法でも精度低下が生じる。この問題は 2004 年、Corless らが指摘した。Corless らは与多項式を巨大根因子と通常根因子に分離する事を提案したが、著者の方法も同じである。異なるのは因子分離に用いる算法だけである：著者は Sasaki-Kako の簡単かつ安定な方法を用いることを提案した。

2) 主係数が巨大な場合も悪条件であることは本著者らが初めて指摘した。この問題を解決するため、本論文は剰余列に付随する余因子列を利用する方法を提案している。

3) この問題は近似 PC-PRS 算法に特有である：算法では剰余列の最後の要素の主係数を与式の主係数の近似 GCD に合わせるのだが、それには主係数による除算が必要だからである。従変数に対して適当な原点移動を行うことでこの問題は簡単に解決できる。

審 査 の 結 果 の 要 旨

近似 GCD は、1989 年に日本で提案されて以来、世界中で 40 近くもの論文が書かれた世界的トピックスである。近似グレブナー基底とともに、今後、幅広い応用分野で用いられるに違いない重要な演算である。その意味で、近似 GCD の計算法の安定化と効率化を目指した著者の研究は重要である。

本論文の第一の点である 1 変数多項式の剰余列算法の安定化については、著者のアイデアは従来の剰余列算法の不安定性に対する明快な考察に基づいており、簡単でありながら一定の効果をもつ点で評価できる。しかし、実験データが示すように、高次多項式に対しては無力なので、この点の改善が強く望まれる。

論文の第二点である多変数多項式の近似 PC-PRS 算法は、世界の多くの研究者が取り組んでいる行列算法

に比して著しく高効率であるため、外国の研究者から高く評価されている。しかし、これは PC-PRS 算法の高効率性をそのまま受け継いだものなので、著者の成果とは言い難い。著者は行列算法のみならず、自身が考案した PC-Givens 法に加えて近似 EZ-GCD 算法もインプリメントして、近似 PC-PRS 算法の優位性を実験的に実証したが、このことは評価できる。

論文の第三点である悪条件問題については、幾つかは本研究で指摘された問題であり、そのことだけでも評価できる。著者の行った工夫はすべて、剰余列算法の観点からのものであるが、悪条件性をかなり克服するものばかりで、高く評価できる。今後、剰余列以外の観点からも悪条件性の克服が望まれる。

よって、著者は博士（理学）の学位を受けるに十分な資格を有するものと認める。